

# A CERTIFICATE FOR SEMIDEFINITE RELAXATIONS IN COMPUTING POSITIVE DIMENSIONAL REAL VARIETIES

YUE MA, CHU WANG AND LIHONG ZHI

**ABSTRACT.** For an ideal  $I$  with a positive dimensional real variety, based on moment relaxations, we study how to compute a Pommaret basis which is simultaneously a Groebner basis of an ideal  $J$  generated by the kernel of a truncated moment matrix and nesting between  $I$  and its real radical ideal. We provide a certificate consisting of a condition on coranks of moment matrices for terminating the algorithm. For a generic delta-regular coordinate system, we prove that the condition is satisfiable in a large enough order of moment relaxations.

## 1. INTRODUCTION

Finding real solutions of a polynomial system is a classical mathematical problem with wide applications. Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{R}[x] := \mathbb{R}[x_1, \dots, x_n]$  be an ideal generated by polynomials  $h_1, \dots, h_m \in \mathbb{R}[x]$ . Its complex and real algebraic varieties are defined as

$$V_{\mathbb{C}}(I) := \{x \in \mathbb{C}^n \mid f(x) = 0 \ \forall f \in I\}, \quad V_{\mathbb{R}}(I) := V_{\mathbb{C}}(I) \cap \mathbb{R}^n.$$

The vanishing ideal of a set  $V \subseteq \mathbb{C}^n$  is an ideal

$$I(V) := \{f \in \mathbb{C}[x] \mid f(v) = 0, \ \forall v \in V\}.$$

The radical (also called complex radical) of  $I$  is

$$\sqrt{I} := \{f \in \mathbb{C}[x] \mid f^k \in I \text{ for some } k \in \mathbb{N}\},$$

while the real radical of  $I$  is defined as

$$\sqrt[\mathbb{R}]{I} := \left\{ f \in \mathbb{R}[x] \mid f^{2k} + \sum_{i=1}^r q_i^2 \in I \text{ for some } k \in \mathbb{N}, q_1, \dots, q_r \in \mathbb{R}[x] \right\}.$$

Clearly, they satisfy the inclusion  $I \subseteq \sqrt{I} \subseteq \sqrt[\mathbb{R}]{I}$ . An ideal  $I$  is called *radical* (resp. *real radical*) if  $I = \sqrt{I}$  (resp.  $I = \sqrt[\mathbb{R}]{I}$ ). According to the Real Nullstellensatz [7], the vanishing ideal  $I(V_{\mathbb{R}}(I))$  of the zero set  $V_{\mathbb{R}}(I)$  is a real radical ideal and  $I(V_{\mathbb{R}}(I)) = \sqrt[\mathbb{R}]{I}$ .

There exists much work on computing a complex radical ideal  $\sqrt{I}$ , like [5, 9, 11, 14, 15]. The algorithms range from numerical ones (e.g., [13, 18, 19]) to symbolic ones (e.g., [6, 31]). For the general case of  $I$  being positive dimensional, a commonly used technique is to reduce the problem to the zero-dimensional case, like in Gianni et al. [11] and Krick and Logar [14].

The problem of computing the real radical ideal  $\sqrt[\mathbb{R}]{I}$  is typically much more difficult than computing  $\sqrt{I}$ . Becker and Neuhaus [4] proposed a symbolic algorithm

<sup>1</sup>KLMM, Academy of Mathematics and Systems Science, CAS, Beijing, 100190, China, {yma, cwang, lzhi}@mmrc.iss.ac.cn

*Key words and phrases.* Real radical ideal, positive dimensional ideal, semidefinite programming, involutive division, Pommaret basis,  $\delta$ -regular.

based on the primary decomposition to compute  $\sqrt[n]{I}$  (also see [25, 34, 39, 40]). Some interesting algorithms based on critical point methods were proposed in [1, 2, 3, 28] to compute a point on each semi-algebraically connected component of real algebraic varieties.

A new approach based on moment relaxations has been proposed by Lasserre et al. [16, 18, 19, 22] for computing  $\sqrt[n]{I}$ , provided it is a zero-dimensional variety. Hereby we briefly describe this interesting approach.

For a sequence  $y = (y_\alpha)_{\alpha \in \mathbb{N}^n} \in \mathbb{R}^{\mathbb{N}^n}$ , its *moment matrix*

$$M(y) := (y_{\alpha+\beta})_{\alpha, \beta \in \mathbb{N}^n}$$

is a real symmetric matrix whose rows and columns are indexed by the set  $\mathbb{T}^n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$  of monomials. Given a polynomial  $h \in \mathbb{R}[x]$ , set  $\text{vec}(h) := (h_\alpha)_{\alpha \in \mathbb{N}^n}$  and define the sequence  $hy := M(y)\text{vec}(h) \in \mathbb{R}^{\mathbb{N}^n}$ . We say that a polynomial  $p$  lies in the kernel of  $M(y)$  when  $M(y)p := M(y)\text{vec}(p) = 0$ . Given a truncated moment sequence  $y = (y_\alpha)_{\alpha \in \mathbb{N}_{2t}^n} \in \mathbb{R}^{\mathbb{N}_{2t}^n}$ , it defines a *truncated moment matrix*

$$M_t(y) := (y_{\alpha+\beta})_{\alpha, \beta \in \mathbb{N}_t^n}$$

indexed by the set  $\mathbb{T}_t^n := \{x^\alpha \mid \alpha \in \mathbb{N}_t^n \text{ with } |\alpha| := \sum_{i=1}^n \alpha_i \leq t\}$ .

We work with the space  $\mathbb{R}[x]_t$  of polynomials of the degree smaller than or equal to  $t$ . For a polynomial  $p \in \mathbb{R}[x]_t$ , if  $M_t(y)\text{vec}(p) = 0$ , we say  $p$  lies in the kernel of  $M_t(y)$ , i.e.,

$$(1) \quad \ker M_t(y) := \{p \in \mathbb{R}[x]_t \mid M_t(y)\text{vec}(p) = 0\}.$$

Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{R}[x]$  be an ideal and set

$$(2) \quad d_j := \lceil \deg(h_j)/2 \rceil, \quad d := \max_{1 \leq j \leq m} d_j.$$

For  $t \geq d$ , define the set

$$(3) \quad \mathcal{K}_t := \{y \in \mathbb{R}^{\mathbb{N}_{2t}^n} \mid y_0 = 1, M_t(y) \succeq 0, M_{t-d_j}(h_j y) = 0, j = 1, \dots, m\}.$$

An element  $y \in \mathcal{K}_t$  is *generic* if  $M_t(y)$  has maximum rank over  $\mathcal{K}_t$ . We denote

$$(4) \quad \mathcal{K}_t^{\text{gen}} := \{y \in \mathcal{K}_t \mid \text{rank } M_t(y) \text{ is maximum over } \mathcal{K}_t\}.$$

When the real algebraic variety  $V_{\mathbb{R}}(I)$  is finite, Lasserre et al.[17] used the flat extension (a rank condition of moment matrices in [8]) as a certificate to check whether polynomials in  $\ker M_s(y)$  ( $1 \leq s \leq t$ ) for a generic element  $y \in \mathcal{K}_t$  generates the real radical ideal  $I(V_{\mathbb{R}}(I))$ . When  $V_{\mathbb{R}}(I)$  is positive dimensional, this certificate does not work. The example given by Fialkow in [10, Example 3.2] can be used to explain the difficulty. Unlike the zero-dimensional case, although the kernel of the moment matrix of the third order consists of only a polynomial  $z - x^3$  which is already a Gröbner basis of the real radical ideal  $I = I(V_{\mathbb{R}}(I)) = \langle z - x^3 \rangle$ , we can not extend the truncated moment sequence  $y \in \mathcal{K}_3$  to the next order, i.e.,  $y$  has no representing measure.

The motivation of this paper is to provide a certificate for checking  $\langle \ker M_t(y) \rangle = I(V_{\mathbb{R}}(I))$  when  $V_{\mathbb{R}}(I)$  is positive dimensional. Unfortunately, we still can not solve this open problem [22, §2.4.3] completely. However, we provide a certificate (10) based on the geometric involutivity theory [29, 30, 33] for checking whether we have obtained a weak Pommaret basis (also a Gröbner basis) of an ideal  $J = \langle \ker M_{t-2}(y) \rangle$  satisfying  $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$  under graded reverse lexicographic order. A (weak) Pommaret basis is a special form of the familiar Gröbner basis which allows for directly reading off the depth, the projective dimension and the

Castelnuovo-Mumford regularity of a module. When the real algebraic variety  $V_{\mathbb{R}}(I)$  is positive dimensional, for examples in Section 4, we succeed in showing that the computed Pommaret basis is an involutive basis of the real radical ideal  $I(V_{\mathbb{R}}(I))$ . In general, it is still not possible to prove that the kernel of the moment matrix satisfying the certificate (10) generates a real radical ideal.

The paper is organized as follows. In Section 2, we review some preliminary backgrounds like elementary algebraic geometry, moment matrices, involutive divisions and involutive bases. In Section 3, we present an algorithm based on the semidefinite programming and moment relaxations in computing a Pommaret basis of an ideal  $J$  satisfying  $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$ ,  $V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n$ , and propose a certificate for terminating the algorithm and prove it works for a positive dimensional  $V_{\mathbb{R}}(I)$  under a  $\delta$ -regular coordinate system. In Section 4, we present computational results for a set of examples in [27, 30, 32, 36]. Some open questions and ongoing work are given in Section 5.

## 2. PRELIMINARY

We introduce some notations and preliminaries about polynomials, matrices, semidefinite programs and the involution. Given  $\mathbb{K} = \mathbb{R}$  or  $\mathbb{C}$ , the ring of multivariate polynomials in  $n$  variables over the field  $\mathbb{K}$  is denoted by  $\mathbb{K}[x] := \mathbb{K}[x_1, \dots, x_n]$ . For an integer  $t \geq 0$ ,  $\mathbb{K}[x]_t$  denotes the set of polynomials of degree at most  $t$ .  $\mathbb{N}$  denotes the set of nonnegative integers and we set  $\mathbb{N}_t^n := \{\alpha \in \mathbb{N}^n \mid |\alpha| := \sum_{i=1}^n \alpha_i \leq t\}$  for  $t \in \mathbb{N}$ . For  $\alpha \in \mathbb{N}^n$ ,  $x^\alpha$  denotes the monomial  $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$  whose total degree is  $|\alpha| := \sum_{i=1}^n \alpha_i$ . All monomials are included in  $\mathbb{T}^n := \{x^\alpha \mid \alpha \in \mathbb{N}^n\}$  and  $\mathbb{T}_t^n := \{x^\alpha \mid \alpha \in \mathbb{N}_t^n\}$  consists of monomials with degrees bounded by  $t \in \mathbb{N}$ . Consider a polynomial  $p \in \mathbb{K}[x]$ ,  $p = \sum_{\alpha \in \mathbb{N}^n} p_\alpha x^\alpha$ , where there are only finitely many nonzero  $p_\alpha \in \mathbb{K}$ , its leading term  $\text{lt}_\prec(p)$  is the maximum term  $x^\alpha$  with respect to a monomial order  $\prec$  for which  $p_\alpha \neq 0$ . We denote by  $\langle \text{lt}_\prec(I) \rangle$  the ideal generated by leading terms of polynomials in  $I$ . The symbol  $[x]_t$  denotes the sequence consisting of all monomials of degrees less than or equal to  $t$ :

$$[x]_t := [1, x_1, \dots, x_n, x_1^2, x_1 x_2, \dots, x_1^t, x_1^{t-1} x_2, \dots, x_n^t].$$

**2.1. Properties of moment matrix.** The kernel of a moment matrix is particularly useful as it has the following properties, see [8, 17, 20, 21, 24].

**Lemma 2.1.** [17, Proposition 3.6] *Let  $\ker M(y) := \{p \in \mathbb{R}[x] \mid M(y)\text{vec}(p) = 0\}$  be the kernel of a moment matrix  $M(y)$ . Then  $\ker M(y)$  is an ideal in  $\mathbb{R}[x]$ . Moreover, if  $M(y) \succeq 0$ , then  $\ker M(y)$  is a real radical ideal.*

The kernel of the truncated moment matrix  $M_t(y)$  is not an ideal, but under certain conditions, it has the following properties.

**Proposition 2.2.** [17, Lemma 3.5, 3.9] *Let  $y \in \mathbb{R}^{\mathbb{N}_{2t}^n}$  and its truncated moment matrix  $M_t(y)$  is positive semidefinite.*

- (i) *If  $f, g \in \mathbb{R}[x]$  with  $\deg(fg) \leq t-1$ , then  $f \in \ker M_t(y) \implies fg \in \ker M_t(y)$ .*
- (ii) *For a polynomial  $p \in \mathbb{R}[x]$ , if  $p^{2k} + \sigma \in \ker M_t(y)$  for some  $k \in \mathbb{N}$  and  $\sigma \in \sum \mathbb{R}[x]^2$ , then  $p \in \ker M_t(y)$ .*
- (iii) *We have  $\ker M_t(y) \cap \mathbb{R}[x]_s = \ker M_s(y)$  for  $1 \leq s \leq t$ .*

Generic elements of  $\mathcal{K}_t$  have useful properties. The following results are cited from [17, Lemma 3.1] and [27, Lemma 7.28, 7.39].

**Proposition 2.3.** *Assume  $y \in \mathcal{K}_t^{gen}$  is generic.*

- (i) *For all  $1 \leq s \leq t$ , we have  $\ker M_s(y) \subseteq \sqrt[s]{I}$  and  $\ker M_s(y) \subseteq \ker M_s(z)$  for all  $z \in \mathcal{K}_t$ .*
- (ii) *If  $t \leq t'$  and  $y' \in \mathcal{K}_{t'}^{gen}$ , then  $\ker M_t(y) \subseteq \ker M_{t'}(y')$ .*
- (iii) *For every finite basis  $\{g_1, \dots, g_k\}$  of the real radical ideal  $\sqrt[s]{I}$ , there exists  $t_0 \in \mathbb{N}$  such that  $g_1, \dots, g_k \in \ker M_t(z)$  for all  $z \in \mathcal{K}_t$  and  $t \geq t_0$ .*
- (iv) *It holds that  $\langle \ker M_t(y) \rangle = \sqrt[s]{I}$  if  $t$  is sufficiently large.*

In the following, we review some properties of moment matrices in the occurrence of inequality constraints. Consider the semialgebraic set

$$(5) \quad \mathcal{A} := \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \dots, f_s(x) \geq 0\},$$

where  $f_1, \dots, f_s \in \mathbb{R}[x]$ . The  $\mathcal{A}$ -variety  $V_{\mathcal{A}}(I)$  denotes the intersection

$$V_{\mathcal{A}}(I) = V_{\mathbb{R}}(I) \cap \mathcal{A}.$$

For every  $\nu \in \{0, 1\}^s$ , we denote the product  $f^\nu := f_1^{\nu_1} f_2^{\nu_2} \cdots f_s^{\nu_s}$ .

**Definition 2.4.** [23] *The  $\mathcal{A}$ -radical of an ideal  $I$  is defined as*

$$\sqrt[\mathcal{A}]{I} := \left\{ p \in \mathbb{R}[x] \mid p^{2k} + \sum_{\nu \in \{0,1\}^s} \sigma_\nu f^\nu \in I \text{ for some } k \in \mathbb{N}, \sigma_\nu \in \sum \mathbb{R}[x]^2 \right\}.$$

*The ideal  $I$  is called  $\mathcal{A}$ -radical if  $I = \sqrt[\mathcal{A}]{I}$ .*

**Theorem 2.5.** [35, Semialgebraic Nullstellensatz] *Let  $I$  be an ideal in  $\mathbb{R}[x]$  and  $\mathcal{A}$  be defined by (5). Then  $\sqrt[\mathcal{A}]{I}$  is an  $\mathcal{A}$ -radical ideal and  $\sqrt[\mathcal{A}]{I} = I(V_{\mathbb{R}}(I) \cap \mathcal{A})$ .*

To compute the  $\mathcal{A}$ -radical ideal  $\sqrt[\mathcal{A}]{I}$ , we consider the set

$$(6) \quad \mathcal{K}_{t,\mathcal{A}} := \mathcal{K}_t \cap \left\{ y \in \mathbb{R}^{\mathbb{N}_{2t}^n} : M_{t-d_f\nu}(f^\nu y) \succeq 0, \forall \nu \in \{0, 1\}^s \right\},$$

where  $d_{f^\nu} = \lceil \deg(f^\nu)/2 \rceil$ . Clearly, the set  $\mathcal{K}_{t,\mathcal{A}}$  is a restriction of  $\mathcal{K}_t$ . The definition of the set  $\mathcal{K}_{t,\mathcal{A}}$  is motivated by the polynomials in  $\sqrt[\mathcal{A}]{I}$  and the Semialgebraic Nullstellensatz. The generic elements of  $\mathcal{K}_{t,\mathcal{A}}$  are similarly defined to be the elements of the set

$$\mathcal{K}_{t,\mathcal{A}}^{gen} := \{y \in \mathcal{K}_{t,\mathcal{A}} : \text{rank } M_t(y) \text{ is maximum over } \mathcal{K}_{t,\mathcal{A}}\}.$$

**Lemma 2.6.** *Let  $\{g_1, \dots, g_k\}$  be a set of generators for the ideal  $\sqrt[\mathcal{A}]{I}$ . Then there exists  $t_0 \in \mathbb{N}$  such that  $g_1, \dots, g_k \in \ker M_t(y)$  for all  $y \in \mathcal{K}_{t,\mathcal{A}}$  and  $t \geq t_0$ .*

The following proof mimics the proof of Claim 4.7 in [17].

*Proof.* For each  $\ell = 1, \dots, k$ , by Theorem 2.5, there exists  $m_\ell \in \mathbb{N}$  and polynomials  $\sigma_\nu \in \sum \mathbb{R}[x]^2$  and  $u_j \in \mathbb{R}[x]$  for  $1 \leq j \leq m$  such that

$$(7) \quad g_\ell^{2m_\ell} + \sum_{\nu \in \{0,1\}^s} \sigma_\nu f^\nu = \sum_{j=1}^m u_j h_j.$$

For  $t \geq t_0$ , where

$$t_0 = 1 + \max(d, \deg(g_\ell^{2m_\ell}), \deg(\sigma_\nu f^\nu), \deg(u_j h_j)),$$

since  $\deg(u_j h_j) \leq t-1$  and  $h_j \in \ker M_t(y)$ , by Proposition 2.2 (i), we have  $u_j h_j \in \ker M_t(y)$ , i.e.,  $g_l^{2m_l} + \sum_{\nu \in \{0,1\}^s} \sigma_\nu f^\nu \in \ker M_t(y)$ . Set  $\sigma_\nu = \sum_j \sigma_{\nu,j}^2 \in \Sigma \mathbb{R}[x]^2$ , then we have

$$\text{vec}(g_l^{m_l})^T M_t(y) \text{vec}(g_l^{m_l}) + \sum_{\nu,j} \text{vec}(\sigma_{\nu,j})^T M_{t-d_{f^\nu}}(f^\nu y) \text{vec}(\sigma_{\nu,j}) = 0.$$

Since  $M_t(y) \succeq 0$  and  $M_{t-d_{f^\nu}}(f^\nu y) \succeq 0$ , every summand in the above expression must be zero, and thus  $g_l^{m_l} \in \ker M_t(y)$ . If  $m_l$  is even,  $g_l^{m_l} \in \ker M_t(y)$  implies  $g_l^{m_l/2} \in \ker M_t(y)$ . If  $m_l$  is odd, since  $\deg(g_l^{m_l+1}) \leq t-1$ , we have

$$g_l^{m_l} \in \ker M_t(y) \Rightarrow g_l^{m_l+1} \in \ker M_t(y) \Rightarrow g_l^{(m_l+1)/2} \in \ker M_t(y).$$

Repeat this process, we can show that  $g_l \in \ker M_t(y)$ .  $\square$

**Theorem 2.7.** *There exists  $t_0 \in \mathbb{N}$  such that  $\langle \ker M_t(y) \rangle = \sqrt[t]{I}$  for all  $y \in \mathcal{K}_{t,\mathcal{A}}^{\text{gen}}$  and  $t \geq t_0$ .*

*Proof.* Let  $\{g_1, \dots, g_k\}$  be a set of generators for the ideal  $\sqrt[t]{I}$ . According to Lemma 2.6, we can choose  $t_0 \in \mathbb{N}$  such that  $g_1, \dots, g_k \in \ker M_t(y)$  for all  $y \in \mathcal{K}_{t,\mathcal{A}}$  and  $t \geq t_0$ . Let  $y \in \mathcal{K}_{t,\mathcal{A}}^{\text{gen}}$  and choose an arbitrary point  $v \in V_{\mathcal{A}}(I)$ . Then  $[v]_{2t} \in \mathcal{K}_{t,\mathcal{A}}$  and  $z = (y + [v]_{2t})/2 \in \mathcal{K}_{t,\mathcal{A}}$ . Clearly, it holds that

$$\ker M_t((y + [v]_{2t})/2) = \ker M_t(y) \cap \ker M_t([v]_{2t}).$$

The rank of  $M_t(y)$  being maximum implies  $\ker M_t((y + [v]_{2t})/2) = \ker M_t(y)$  and  $\ker M_t(y) \subseteq \ker M_t([v]_{2t})$ . For every  $p \in \ker M_t(y)$ , we must have  $p \in \ker M_t([v]_{2t})$  and  $p(v) = 0$ . This means that  $p$  vanishes on the set  $V_{\mathcal{A}}(I)$ . By Theorem 2.5, we get  $p \in \sqrt[t]{I}$  and thus the inclusion  $\langle \ker M_t(y) \rangle \subseteq \sqrt[t]{I} = I(V_{\mathcal{A}}(I))$  holds. Since  $g_1, \dots, g_k \in \ker M_t(y)$ , we get  $\langle \ker M_t(y) \rangle \supseteq \sqrt[t]{I} = I(V_{\mathcal{A}}(I))$  and the proof is completed.  $\square$

**2.2. Involutive Divisions and Involutive Bases.** When the real algebraic variety  $V_{\mathbb{R}}(I)$  is finite, Lasserre et al. [16, 17] proposed new approaches based on moment relaxations for computing Gröbner bases or border bases of the real radical ideal  $\sqrt[\mathbb{R}]{I}$ . For the positive dimensional real variety  $V_{\mathbb{R}}(I)$ , we can also compute its Gröbner bases. Stimulated by the work in [18] and [26, 29, 30], we propose a new approach based on the completion to involution to compute a Pommaret basis of an ideal nested between  $I$  and  $\sqrt[\mathbb{R}]{I}$ . A Pommaret basis is simultaneously a Gröbner basis, but contains extra information such as the Castelnuovo-Mumford regularity. Moreover, we provide a new stopping criterion for the algorithm which is based on the classical Cartan's test for involution from the theory of exterior differential systems. We now introduce some basic concepts from the classical theory of involutive systems for polynomial systems. For background, see [32, 33].

**Definition 2.8.** *Let  $\nu = [\nu_1, \dots, \nu_n] \in \mathbb{N}^n$  be the multi index of a monomial  $x^\nu$ . If  $k$  is the smallest value such that  $\nu_k \neq 0$ , then the class of  $\nu$  or  $x^\nu$  is  $k$ , written by  $\text{cls}(\nu) = k$  or  $\text{cls}(x^\nu) = k$ . The class of a polynomial  $f$  which is denoted by  $\text{cls}(f)$  is  $k$ , if the class of its leading term  $\text{cls}(\text{lt}_{\prec}(f)) = k$ .*

We say that a term order *respects classes*, if for monomials  $x^\mu$  and  $x^\nu$  of the same total degree,  $\text{cls}(\mu) < \text{cls}(\nu)$  implies  $x^\mu \prec x^\nu$ . An important example of a class respecting ordering is the *graded reverse lexicographic* order  $\prec_{\text{tdeg}}$ .

**Definition 2.9.** With an ordering on the variables  $x_1 \prec \cdots \prec x_n$ , the graded reverse lexicographic order  $\prec_{\text{tdeg}}$  is defined by  $x^\alpha \prec_{\text{tdeg}} x^\beta$ , if  $|\alpha| < |\beta|$ , or  $|\alpha| = |\beta|$  and the first non-vanishing entry of the multi index  $\alpha - \beta$  is positive.

Throughout the paper, we use  $\prec_{\text{tdeg}}$  in assigning orders of monomials, and sorting rows and columns of a moment matrix  $M_t(y)$ . Let  $(\mathbb{N}^n, +)$  be an Abelian monoid with the addition defined componentwise. For any multi index  $\nu \in \mathbb{N}^n$ , we introduce its cone  $\mathcal{C}(\nu) = \nu + \mathbb{N}^n$ , i.e., the set of all multi indices that can be reached from  $\nu$  by adding another multi index.

**Definition 2.10.** [33, Definition 3.1.1] An involutive division  $L$  is defined on the monoid  $(\mathbb{N}^n, +)$ , if for any finite subset  $\mathcal{B} \subset \mathbb{N}^n$ , a set  $N_{L,\mathcal{B}}(\nu) \subseteq \{1, \dots, n\}$  of multiplicative indices, and consequently a submonoid  $L(\nu, \mathcal{B}) = \{\mu \in \mathbb{N}^n \mid \forall j \notin N_{L,\mathcal{B}}(\nu) : \mu_j = 0\}$ , is associated to every multi index  $\nu \in \mathcal{B}$  such that the following two conditions on the involutive cones  $\mathcal{C}_{L,\mathcal{B}}(\nu) = \nu + L(\nu, \mathcal{B}) \subseteq \mathbb{N}^n$  are satisfied.

- (i) If there exist two elements  $\mu, \nu \in \mathcal{B}$  with  $\mathcal{C}_{L,\mathcal{B}}(\mu) \cap \mathcal{C}_{L,\mathcal{B}}(\nu) \neq \emptyset$ , either  $\mathcal{C}_{L,\mathcal{B}}(\mu) \subseteq \mathcal{C}_{L,\mathcal{B}}(\nu)$  or  $\mathcal{C}_{L,\mathcal{B}}(\nu) \subseteq \mathcal{C}_{L,\mathcal{B}}(\mu)$  holds.
- (ii) If  $\mathcal{B}' \subset \mathcal{B}$ , then  $N_{L,\mathcal{B}}(\nu) \subseteq N_{L,\mathcal{B}'}(\nu)$  for all  $\nu \in \mathcal{B}'$ .

An arbitrary multi index  $\mu \in \mathbb{N}^n$  is involutively divisible by  $\nu \in \mathcal{B}$ , written  $\nu \mid_{L,\mathcal{B}} \mu$ , if  $\mu \in \mathcal{C}_{L,\mathcal{B}}(\nu)$ . In this case  $\nu$  is called an involutive divisor of  $\mu$ .

**Definition 2.11.** [33, Example 3.1.7] The Pommaret division written by  $P$  is defined by a simple rule: if  $\text{cls}(\nu) = k$ , then we set  $N_{L,\mathcal{B}}(\nu) = \{1, \dots, k\}$ .

**Remark 2.12.** The Pommaret division is a globally defined division as the assignment of the multiplicative indices to a multi index  $\nu \in \mathcal{B}$  is independent of the set  $\mathcal{B}$ . The Pommaret division is an involutive division by [33, Lemma 3.1.8].

**Definition 2.13.** [33, Definition 3.1.9] The involutive span of a finite set  $\mathcal{B} \subset \mathbb{N}^n$  is

$$(8) \quad \langle \mathcal{B} \rangle_L = \bigcup_{\nu \in \mathcal{B}} \mathcal{C}_{L,\mathcal{B}}(\nu).$$

The set  $\mathcal{B}$  is called weakly involutive for the division  $L$  or a weak involutive basis of the monoid ideal  $\langle \mathcal{B} \rangle$ , if  $\langle \mathcal{B} \rangle_L = \langle \mathcal{B} \rangle$ . The set  $\mathcal{B}$  is a strong involutive basis or for short an involutive basis, if the union (8) is disjoint, i.e., the intersections of the involutive cones are empty.

For a polynomial  $f \in \mathbb{K}[x]$  and a term order  $\prec$ , we select its leading term  $\text{lt}_\prec(f) = x^\mu$  with the leading exponent  $\text{le}_\prec(f) = \mu$ .

**Definition 2.14.** [33, Definition 3.4.1] Let  $I \subseteq \mathbb{K}[x]$  be an ideal. A finite set  $\mathcal{H} \subset I$  is a weak involutive basis of  $I$  for an involutive division  $L$  on  $\mathbb{N}^n$ , if  $\text{le}_\prec(\mathcal{H})$  is a weak involutive basis of the monoid ideal  $\text{le}_\prec(I)$ . The set  $\mathcal{H}$  is a strong involutive basis of  $I$ , if  $\text{le}_\prec(\mathcal{H})$  is a strong involutive basis of  $\text{le}_\prec(I)$  and two distinct elements of  $\mathcal{H}$  never possess the same leading exponents.

**Remark 2.15.** Definition 2.13 and Definition 2.14 imply immediately that any weak involutive basis is a Gröbner basis.

Not every ideal in  $\mathbb{K}[x]$  possesses a finite Pommaret basis (see [33]).

**Definition 2.16.** [33, Definition 4.3.1] A coordinate system is called  $\delta$ -regular for the ideal  $I \subseteq \mathbb{K}[x]$  and the term order  $\prec$ , if  $I$  possesses a finite Pommaret basis for the term order  $\prec$ .

**Theorem 2.17.** [33, Theorem 4.3.15] *Every polynomial ideal  $I \subseteq \mathbb{K}[x]$  possesses a finite Pommaret basis for a term order  $\prec$  in suitably chosen coordinate systems.*

**Definition 2.18.** [33, Definition 3.4.2] *Let  $\mathcal{F} \subset \mathbb{K}[x] \setminus \{0\}$  be a finite set of polynomials and  $L$  be an involutive division on  $\mathbb{N}^n$ . We assign to each element  $f \in \mathcal{F}$  a set of multiplicative variables*

$$X_{L,\mathcal{F},\prec}(f) = \{x_i \mid i \in N_{L,\text{le}_\prec \mathcal{F}}(\text{le}_\prec f)\}.$$

*The involutive span of  $\mathcal{F}$  is then the set*

$$\langle \mathcal{F} \rangle_{L,\prec} = \sum_{f \in \mathcal{F}} \mathbb{K}[X_{L,\mathcal{F},\prec}(f)] \cdot f \subseteq \langle \mathcal{F} \rangle.$$

**Theorem 2.19.** [33, Theorem 3.4.4] *Let  $I \subseteq \mathbb{K}[x]$  be a nonzero ideal,  $\mathcal{H} \subset I \setminus \{0\}$  a finite set and  $L$  an involutive division on  $\mathbb{N}^n$ . Then the following two statements are equivalent.*

- (i) *The set  $\mathcal{H} \subset I$  is a weak involutive basis of  $I$  with respect to  $L$  and  $\prec$ .*
- (ii) *Every polynomial  $f \in I$  can be written in the form*

$$(9) \quad f = \sum_{h \in \mathcal{H}} P_h \cdot h$$

*with coefficients  $P_h \in \mathbb{K}[X_{L,\mathcal{H},\prec}(h)]$  satisfying  $\text{lt}_\prec(P_h \cdot h) \preceq \text{lt}_\prec(f)$  for all polynomials  $h \in \mathcal{H}$  such that  $P_h \neq 0$ .*

*$\mathcal{H}$  is a strong involutive basis, if and only if the representation (9) is unique.*

**Corollary 2.20.** [33, Corollary 3.4.5] *Let  $\mathcal{H}$  be a weak involutive basis of the ideal  $I \subseteq \mathbb{K}[x]$ . Then  $\langle \mathcal{H} \rangle_{L,\prec} = I$ . If  $\mathcal{H}$  is even a strong involutive basis of  $I$ , then  $I$  considered as a  $\mathbb{K}$ -linear space possesses a direct sum decomposition  $I = \bigoplus_{h \in \mathcal{H}} \mathbb{K}[X_{L,\mathcal{H},\prec}(h)] \cdot h$ .*

**Proposition 2.21.** [33, Proposition 3.4.7] *Let  $I \subseteq \mathbb{K}[x]$  be an ideal and  $\mathcal{H} \subset I$  be a weak involutive basis of  $I$  for the involutive division  $L$ . Then there exists a subset  $\mathcal{H}' \subseteq \mathcal{H}$  which is a strong involutive basis of  $I$ .*

**Definition 2.22.** *If we regard  $\mathbb{K}[x]$  as a linear space, then the ideal  $I$  and the truncated ideal  $I_t = I \cap \mathbb{K}[x]_t$  are both subspaces in  $\mathbb{K}[x]$ . We say that the set  $G = \{g_1, \dots, g_s\}$  is a reduced basis of  $I_t$ , if it is a linear independent basis of  $I_t$  and all polynomials in  $G$  have different leading monomials with respect to a given term order.*

### 3. COMPUTING A POMMARET BASIS

In this section, we present an algorithm as well as a certificate for computing a Pommaret basis for an ideal  $J$ , s.t.  $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$  when  $V_{\mathbb{R}}(I)$  is positive dimensional. The certificate given in (10) generalizes the flat extension conditions in [17] for the zero-dimensional real variety to the positive dimensional case.

**3.1. The certificate.** Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{R}[x]$  be an ideal and  $d := \max_{1 \leq j \leq m} d_j$ ,  $d_j := \lceil \deg(h_j)/2 \rceil$ . For each  $t \geq d$ , recall the notions

$$\mathcal{K}_t := \{y \in \mathbb{R}^{\mathbb{N}_{2t}^n} \mid y_0 = 1, M_t(y) \succeq 0, M_{t-d_j}(h_j y) = 0, j = 1, \dots, m\},$$

and

$$\mathcal{K}_t^{gen} := \{y \in \mathcal{K}_t \mid \text{rank } M_t(y) \text{ is maximum over } \mathcal{K}_t\}.$$

For a moment matrix  $M_t(y)$  of order  $t$ , the truncated moment matrix  $M_{t-\ell}(y)$  for  $\ell < t$  is the order  $t - \ell$  principal submatrix of  $M_t(y)$  indexed by  $\alpha, \beta \in \mathbb{N}_{t-\ell}^n$ .

Let  $\alpha_j$  denote the number of class  $j$  polynomials of degree  $t - 2$  in the reduced basis of  $\ker M_{t-2}(y)$ . We have the following theorem:

**Theorem 3.1.** *Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{R}[x]$  be an ideal. If there exists an integer  $t \geq 2d$  satisfying*

$$(10) \quad \sum_{j=1}^n j \alpha_j \text{ for } \ker M_{t-2}(y) = \text{corank } M_{t-1}(y) - \text{corank } M_{t-2}(y),$$

*for an element  $y \in \mathcal{K}_t^{gen}$ . Then a reduced basis of the null space of  $M_{t-2}(y)$  is a weak Pommaret basis for  $J = \langle \ker M_{t-2}(y) \rangle$  under the monomial ordering  $\prec_{\text{tdeg}}$  and*

$$(11) \quad I \subseteq \langle J \rangle \subseteq I(V_{\mathbb{R}}(I)), \quad V_{\mathbb{R}}(I) = V_{\mathbb{C}}(J) \cap \mathbb{R}^n.$$

The proof of Theorem 3.1 follows from Proposition 2.3 and Theorem 3.9 whose proofs are given in Section 3.3.

**Remark 3.2.** Although the reduced bases of  $\ker M_{t-2}(y)$  are not unique, they have the same set of leading terms since they can be represented linearly by each other. Therefore, each reduced basis of  $\ker M_{t-2}(y)$  has the same value of  $\sum_{j=1}^n j \alpha_j$ .

In our algorithm, we need to find an element  $y$  in  $\mathcal{K}_t$  maximizing the rank of  $M_t(y)$ . As pointed out in [17], this could be done typically by solving the semidefinite program

$$(12) \quad \min \quad 0 \quad \text{s.t.} \quad y \in \mathcal{K}_t$$

with interior-point algorithms using self-dual embedding, see [37, 38].

**3.2. An algorithm for computing a Pommaret basis.** We list main steps of our algorithm based on solving (12) for computing a Pommaret basis of the ideal  $J = \langle \ker M_{t-2}(y) \rangle$  nested between  $I$  and  $I(V_{\mathbb{R}}(I))$ .

**Algorithm 3.3.** Computing a Pommaret basis of an ideal  $J$  such that  $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$ .

**Input:** A set of polynomials  $\{h_1, \dots, h_m\}$  generating  $I$  and the monomial ordering  $\prec_{\text{tdeg}}$  on variables  $x_1, \dots, x_n$ .

**Output:** A Pommaret basis for  $\langle \ker M_{t-2}(y) \rangle$  under the monomial ordering  $\prec_{\text{tdeg}}$ .

**Step 1:** For  $t \geq 2d$ , compute a generic element  $y \in \mathcal{K}_t$  by solving (12).

**Step 2:** Compute a reduced basis of  $\ker M_{t-1}(y)$ . Let  $\{g_1, \dots, g_{s+t}\}$  be polynomials of degree  $t-2$  in this reduced basis. Compute the value of  $\sum_{j=1}^n j \alpha_j$ .

**Step 3:** Compute  $\text{corank } M_{t-1}(y) - \text{corank } M_{t-2}(y)$  by calculating the number of polynomials of degree  $t-1$  in the reduced basis of  $\ker M_{t-1}(y)$ .

**Step 4:** Test whether the condition (10) is satisfied.



- If yes,  $\{g_1, \dots, g_{s+r}\}$  is a weak Pommaret basis for  $\langle \ker M_{t-2}(y) \rangle$  and can be reduced further to a (strong) Pommaret basis.
- Otherwise, let  $t := t + 1$  and go to Step 1.

In Section 3.3, we prove that Algorithm 3.3 is correct and terminates in a finite number of steps in a  $\delta$ -regular coordinate system for  $\sqrt[t]{I}$ . The algorithm has been implemented in Matlab using the GloptiPoly toolbox [12] and we demonstrate its performance on a set of examples in Section 4.

**Remark 3.4.** In order to check the condition (10), we need to compute a reduced basis of the null space of the truncated moment matrix  $M_{t-1}(y)$ . These computations have to be performed stably. For the computation of a reduced basis it is important to choose a proper tolerance to ensure that there is no information missing in  $\ker M_{t-1}(y)$ . We list the tolerance used for each example in Section 4.

**3.3. Justification of the certificate.** Our main goal in this section is to prove that Algorithm 3.3 is correct and it terminates after a finite number of steps in a  $\delta$ -regular coordinate system for  $\sqrt[t]{I}$ .

**Assumption 3.5.** Let  $I = \langle h_1, \dots, h_m \rangle \subseteq \mathbb{R}[x]$  be an ideal. Suppose there exists an integer  $t \geq 2d$  satisfying the condition (10) for  $y \in \mathcal{K}_t^{gen}$ . Let  $\{g_1, \dots, g_{s+r}\}$  be a reduced basis of  $\ker M_{t-2}(y)$ , where

$$\deg(g_i) = t - 2 \text{ for } 1 \leq i \leq s, \text{ and } \deg(g_i) < t - 2 \text{ for } s + 1 \leq i \leq s + r.$$

**Lemma 3.6.** Under Assumption 3.5, the polynomial set

$$\{x_1 g_1, \dots, x_{j_1} g_1, \dots, x_1 g_s, \dots, x_{j_s} g_s, g_1, \dots, g_{s+r}\}$$

is a reduced basis of  $\ker M_{t-1}(y)$ , where  $j_i = \text{cls}(g_i)$  for  $i = 1, \dots, s$ .

*Proof.* For  $k = 1, \dots, n$ ,  $i = 1, \dots, s + r$ , since  $\deg(x_k g_i) \leq t - 1$ , by Proposition 2.2 (i), we have  $x_k g_i \in \ker M_{t-1}(y)$ . In fact, since each polynomial in  $\{g_1, \dots, g_{s+r}\}$  has different leading terms, according to Definition 2.10, the polynomials

$$(13) \quad x_1 g_1, \dots, x_{j_1} g_1, \dots, x_1 g_s, \dots, x_{j_s} g_s$$

all have distinct leading terms of degree  $t - 1$ . Hence they are linearly independent. Suppose there are  $\alpha_j$  polynomials of class  $j$  in  $\{g_1, \dots, g_s\}$ , then polynomials in (13) yield  $\sum_{j=1}^n j \alpha_j$  linearly independent polynomials of degree  $t - 1$  in  $\ker M_{t-1}(y)$ . On the other hand, the number of linearly independent polynomials of degree  $t - 1$  in a reduced basis of  $\ker M_{t-1}(y)$  equals to  $\text{corank } M_{t-1}(y) - \text{corank } M_{t-2}(y)$ . Hence, the condition (10) and Proposition 2.2 (iii) implies that the conclusion is true.  $\square$

**Remark 3.7.** Under Assumption 3.5, for any polynomial  $f \in \ker M_{t-1}(y)$ , we can express it as a linear combination:

$$(14) \quad f = \sum_{k=1}^s \sum_{i=1}^{\text{cls}(g_k)} c_{ik} x_i g_k + \sum_{k=1}^{s+r} \lambda_k g_k,$$

where  $c_{ik} \in \mathbb{R}$  and  $\text{lt}_{\prec}(c_{ik} x_i g_k) \preceq_{\text{tdeg}} \text{lt}_{\prec}(f)$  for  $1 \leq i \leq \text{cls}(g_k)$  and  $1 \leq k \leq s$ ,  $\lambda_k \in \mathbb{R}$  and  $\text{lt}_{\prec}(\lambda_k g_k) \preceq_{\text{tdeg}} \text{lt}_{\prec}(f)$  for  $1 \leq k \leq s + r$ . Note that every polynomial in  $\{x_1 g_1, \dots, x_{j_1} g_1, \dots, x_1 g_s, \dots, x_{j_s} g_s, g_1, \dots, g_{s+r}\}$  has a different leading term. Under the graded monomial ordering  $\prec_{\text{tdeg}}$ , there is only one  $c_{i_0 k_0} \neq 0$  with  $\text{lt}_{\prec}(x_{i_0} g_{k_0}) = \text{lt}_{\prec}(f)$  if not all  $c_{ik}$  are zeros. This property is very important and will be used in the proofs of theorems below.

**Lemma 3.8.** *Under Assumption 3.5, for all monomial  $x^\mu$  and polynomials  $g_j$  with  $\deg(g_j) < t - 2$ ,  $j = s + 1, \dots, s + r$ , the polynomial  $x^\mu g_j$  can be expressed as*

$$(15) \quad x^\mu g_j = \sum_{k=1}^s h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k g_k,$$

where  $h_k \in \mathbb{R}[x]$  and  $\lambda_k \in \mathbb{R}$  satisfying  $\text{lt}_<(h_k g_k) \preceq_{\text{tdeg}} \text{lt}_<(x^\mu g_j)$ ,  $k = 1, \dots, s$  and  $\text{lt}_<(\lambda_k g_k) \preceq_{\text{tdeg}} \text{lt}_<(x^\mu g_j)$ ,  $k = s + 1, \dots, s + r$ .

*Proof.* If  $\deg(x^\mu g_j) \leq t - 1$ , by Proposition 2.2 (i), we have  $x^\mu g_j \in \ker M_{t-1}(y)$ . According to Remark 3.7, we have the expression (15). Otherwise, we set  $x^\mu = x^{\mu_1} x^{\mu_2}$  such that  $\deg(x^{\mu_2} g_j) = t - 1$ . Hence, we have

$$\begin{aligned} x^\mu g_j &= x^{\mu_1} x^{\mu_2} g_j = x^{\mu_1} \left( \sum_{k=1}^s h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k g_k \right) \\ &= \sum_{k=1}^s x^{\mu_1} h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k x^{\mu_1} g_k. \end{aligned}$$

We can repeat the above reduction on  $x^{\mu_1} g_k$  for  $s + 1 \leq k \leq s + r$ . Since  $\deg(x^{\mu_1}) < \deg(x^\mu)$ , after a finite number of steps, we have the expected form (15).  $\square$

**Theorem 3.9.** *Under Assumption 3.5, a reduced basis  $\{g_1, \dots, g_{s+r}\}$  of  $\ker M_{t-2}(y)$  is a weak Pommaret basis of the ideal  $\langle \ker M_{t-2}(y) \rangle$ .*

*Proof.* We show that any polynomial  $f \in \langle \ker M_{t-2}(y) \rangle$  can be represented as

$$(16) \quad f = \sum_{k=1}^s h_k g_k + \sum_{k=s+1}^{s+r} \lambda_k g_k,$$

where  $\lambda_k \in \mathbb{R}$  and  $h_k \in \mathbb{R}[x_1, \dots, x_{\text{cls}(g_k)}]$ . Since  $\text{lt}_<(h_k g_k)$  and  $\text{lt}_<(g_k)$  are all different for  $1 \leq k \leq s + r$ , if  $f$  satisfies (16), then we have  $\text{lt}_<(h_k g_k) \preceq_{\text{tdeg}} \text{lt}_<(f)$  for  $1 \leq k \leq s$  and  $\text{lt}_<(\lambda_k g_k) \preceq_{\text{tdeg}} \text{lt}_<(f)$  for  $s + 1 \leq k \leq s + r$ . Therefore, according to Theorem 2.19, the polynomial set  $\{g_1, \dots, g_{s+r}\}$  is a weak Pommaret basis of the ideal  $\langle \ker M_{t-2}(y) \rangle$ .

Since  $\{g_1, \dots, g_{s+r}\}$  is a reduced basis of  $\ker M_{t-2}(y)$ , every polynomial  $f \in \langle \ker M_{t-2}(y) \rangle$  can be represented as

$$f = \sum_{j=1}^{s+r} h_j g_j,$$

where  $h_j \in \mathbb{R}[x]$ ,  $j = 1, \dots, s + r$ . Hence, we only need to show that each polynomial  $x^\mu g_j$  for  $\mu \in \mathbb{N}^n$  and  $1 \leq j \leq s + r$  can be written as (16).

Set  $f = x^\mu g_j$ . If  $\deg(f) \leq t - 1$ , by Lemma 3.6, we have the expected expression (16) directly. Otherwise, we prove by the induction on its leading term  $\text{lt}_<(f) = t_0$ , i.e., we assume that  $f = x^\mu g_j$  has the expected expression (16) as long as  $\text{lt}_<(f) \prec_{\text{tdeg}} t_0$  for  $\mu \in \mathbb{N}^n$  and  $1 \leq j \leq s + r$ , we show it has the expected expression when  $\text{lt}_<(f) = t_0$ .

If  $x^\mu \in \mathbb{R}[x_1, \dots, x_{\text{cls}(g_j)}]$ , nothing is to be proved. Otherwise, without loss of generality, let  $x_{i_1}$  be a non-multiplicative variable in  $x^\mu$  with respect to  $g_j$ . Since

$\deg(g_j) \leq t-2$ ,  $j = 1, \dots, s+r$ , by Proposition 2.2 (i), we have  $x_{i_1}g_j \in \ker M_{t-1}(y)$ . By Lemma 3.6 and Remark 3.7, we have

$$\begin{aligned}
 f &= x^\mu g_j = (x^\mu/x_{i_1}) x_{i_1} g_j \\
 &= (x^\mu/x_{i_1}) \left( \sum_{k=1}^s \sum_{i=1}^{\text{cls}(g_k)} c_{ik} x_i g_k + \sum_{k=1}^{s+r} \lambda_k g_k \right) \\
 (17) \quad &= \sum_{k=1}^s \sum_{i=1}^{\text{cls}(g_k)} c_{ik} (x^\mu/x_{i_1}) x_i g_k + \sum_{k=1}^{s+r} \lambda_k (x^\mu/x_{i_1}) g_k.
 \end{aligned}$$

According to Remark 3.7, there are two cases:

- (i) if all  $c_{ik} = 0$ , there exists only one  $1 \leq j_1 \leq s+r$ , such that  $\lambda_{j_1} \neq 0$  and  $\text{lt}_{\prec}(\lambda_{j_1} (x^\mu/x_{i_1}) g_{j_1}) = t_0$ ;
- (ii) otherwise, there exists  $1 \leq j_1 \leq s$  and  $1 \leq i_2 \leq \text{cls}(g_{j_1})$  such that  $c_{i_2 j_1} \neq 0$  and  $\text{lt}_{\prec}(c_{i_2 j_1} (x^\mu/x_{i_1}) x_{i_2} g_{j_1}) = t_0$ .

In both cases, all other terms in (17) have leading terms of order less than  $t_0$ , which can be expressed as (16) by induction. Moreover, above two cases do not exist simultaneously. Therefore, we only need to check whether the polynomial  $\lambda_{j_1} (x^\mu/x_{i_1}) g_{j_1}$  in case (i) or  $c_{i_2 j_1} (x^\mu/x_{i_1}) x_{i_2} g_{j_1}$  in case (ii) has the representation (16).

In case (i), if  $x^\mu/x_{i_1} \in \mathbb{R}[x_1, \dots, x_{\text{cls}(g_{j_1})}]$  then we obtain the representation (16). Otherwise, we repeat the reduction to the polynomial  $(x^\mu/x_{i_1}) g_{j_1}$ . Since  $\text{lt}_{\prec}(\lambda_{j_1} (x^\mu/x_{i_1}) g_{j_1}) = \text{lt}_{\prec}(x^\mu g_j) = t_0$ , we have  $\deg(g_j) < \deg(g_{j_1})$ , i.e.,

$$\text{lt}_{\prec}(g_j) \prec_{\text{tdeg}} \text{lt}_{\prec}(g_{j_1}).$$

In case (ii), if  $x^\mu/x_{i_1} \in \mathbb{R}[x_1, \dots, x_{\text{cls}(g_{j_1})}]$ , since  $x_{i_2}$  is a multiplicative variable of  $\text{lt}_{\prec}(g_{j_1})$ , then  $(x^\mu/x_{i_1}) x_{i_2} \in \mathbb{R}[x_1, \dots, x_{\text{cls}(g_{j_1})}]$ . Hence, we obtain the representation (16). Otherwise, since  $x_{i_1}$  is a non-multiplicative variable of  $\text{lt}_{\prec}(g_j)$  and  $x_{i_2}$  is a multiplicative variable of  $\text{lt}_{\prec}(g_{j_1})$ , we have

$$\text{cls}(g_j) < \text{cls}(x_{i_1}), \quad \text{cls}(x_{i_2}) \leq \text{cls}(g_{j_1}).$$

Because  $\text{lt}_{\prec}(c_{i_2 j_1} (x^\mu/x_{i_1}) x_{i_2} g_{j_1}) = t_0$ , we have  $\text{lt}_{\prec}(x_{i_2} g_{j_1}) = \text{lt}_{\prec}(x_{i_1} g_j)$  and

$$(18) \quad \text{cls}(x_{i_2}) = \text{cls}(x_{i_2} g_{j_1}) = \text{cls}(x_{i_1} g_j) < \text{cls}(x_{i_1}).$$

This implies that  $x_{i_2} \prec_{\text{tdeg}} x_{i_1}$ . If  $\text{lt}_{\prec}(g_{j_1}) \preceq_{\text{tdeg}} \text{lt}_{\prec}(g_j)$ , we have  $\text{lt}_{\prec}(x_{i_2} g_{j_1}) \prec_{\text{tdeg}} \text{lt}_{\prec}(x_{i_1} g_j)$  which leads to a contradiction. Therefore, we can deduce that

$$\text{lt}_{\prec}(g_j) \prec_{\text{tdeg}} \text{lt}_{\prec}(g_{j_1}).$$

In both cases, if the reduction does not stop, we will obtain a sequence of polynomials satisfying

$$\text{lt}_{\prec}(g_j) \prec_{\text{tdeg}} \text{lt}_{\prec}(g_{j_1}) \prec_{\text{tdeg}} \dots \prec_{\text{tdeg}} \text{lt}_{\prec}(g_{j_i}) \prec_{\text{tdeg}} \text{lt}_{\prec}(g_{j_{i+1}}) \prec_{\text{tdeg}} \dots \prec_{\text{tdeg}} t_0.$$

Since the number of polynomials with strict increase leading terms bounded by  $\text{lt}_{\prec}(f) = t_0$  is finite, the above procedure will stop in a finite number of steps and we obtain the expected form (16) for  $f$ .  $\square$

**Theorem 3.10.** *In a  $\delta$ -regular coordinate system for  $\sqrt[\mathbb{R}]{I}$ , after a finite number of steps, Algorithm 3.3 will terminate and return an integer  $t \geq 2d$  which satisfies the condition (10) for an element  $y \in \mathcal{K}_t^{\text{gen}}$ .*

*Proof.* In a  $\delta$ -regular coordinate system, we have a finite Pommaret basis  $\mathcal{H} = \{h_1, \dots, h_s\}$  for the real radical ideal  $I(V_{\mathbb{R}}(I))$ . According to Proposition 2.3 (iii), we can conclude that there exists an integer  $t_1$  such that the Pommaret basis  $\{h_1, \dots, h_s\}$  is contained in  $\ker M_t(y)$  for all  $y \in \mathcal{K}_t$  and  $t \geq t_1$ .

Since  $\mathcal{H}$  is a Pommaret basis of  $I(V_{\mathbb{R}}(I))$ , according to Corollary 2.20, for  $t \geq t_1 + 2$ , we have the following decomposition:

$$(19) \quad I(V_{\mathbb{R}}(I))_{t-2} = \bigoplus_{h_k \in \mathcal{H}} \mathbb{R}[x_1, \dots, x_{\text{cls}(h_k)}]_{t-2-\deg(h_k)} \cdot h_k.$$

Let

$$(20) \quad T = \{x^u h_k \mid x^u \in \mathbb{R}[x_1, \dots, x_{\text{cls}(h_k)}], \deg(x^u) \leq t-2-\deg(h_k), 1 \leq k \leq s\}.$$

According to Proposition 2.2 (i),  $T \subseteq \ker M_{t-2}(y)$ . Therefore, by (19) and (20), we have

$$I(V_{\mathbb{R}}(I))_{t-2} \subseteq \ker M_{t-2}(y).$$

On the other hand,  $y$  is a generic element, by Proposition 2.3 (i), we have

$$\ker M_{t-2}(y) \subseteq I(V_{\mathbb{R}}(I))_{t-2}.$$

Hence, we have  $\ker M_{t-2}(y) = I(V_{\mathbb{R}}(I))_{t-2}$  and the decomposition:

$$(21) \quad \ker M_{t-2}(y) = \bigoplus_{h_k \in \mathcal{H}} \mathbb{R}[x_1, \dots, x_{\text{cls}(h_k)}]_{t-2-\deg(h_k)} \cdot h_k.$$

Since  $\mathcal{H}$  is a Pommaret basis of  $I(V_{\mathbb{R}}(I))$ , according to Definition 2.14, each polynomial in  $T$  has a different leading term. Therefore  $T$  is actually a reduced basis of  $\ker M_{t-2}(y)$ . By Remark 3.2, it suffices to show that the condition (10) holds for the polynomials in  $T$ .

Similar to the decomposition (21), we can show that there exists a direct sum decomposition of  $\ker M_{t-1}(y)$ :

$$(22) \quad \ker M_{t-1}(y) = \bigoplus_{h_k \in \mathcal{H}} \mathbb{R}[x_1, \dots, x_{\text{cls}(h_k)}]_{t-1-\deg(h_k)} \cdot h_k.$$

For a polynomial  $f \in \ker M_{t-1}(y)$  with  $\deg(f) = t-1$ , according to (22), we have the following equalities:

$$\begin{aligned} f &= \sum_{k=1}^s \sum_{0 \leq |\mu| \leq t-1-\deg(h_k)} c_{\mu k} x^{\mu} h_k \quad (\text{note that } x^{\mu} \in \mathbb{R}[x_1, \dots, x_{\text{cls}(h_k)}]) \\ &= \sum_{k=1}^s \sum_{|\mu|=t-1-\deg(h_k)} c_{\mu k} x^{\mu} h_k + \sum_{k=1}^s \sum_{0 \leq |\mu| \leq t-2-\deg(h_k)} c_{\mu k} x^{\mu} h_k \\ &= \sum_{k=1}^s \sum_{|\mu|=t-1-\deg(h_k)} c_{\mu k} x_{\text{cls}(x^{\mu})} (x^{\mu}/x_{\text{cls}(x^{\mu})}) h_k + \sum_{k=1}^s \sum_{0 \leq |\mu| \leq t-2-\deg(h_k)} c_{\mu k} x^{\mu} h_k. \end{aligned}$$

Since  $x_{\text{cls}(x^{\mu})}$  is always a multiplicative variable for the polynomial  $(x^{\mu}/x_{\text{cls}(x^{\mu})}) h_k \in T$ , we know that each polynomial in  $\ker M_{t-1}(y)$  can be represented by the polynomials in  $T$  and  $T_1$ , where

$$T_1 = \{x_i g \mid 1 \leq i \leq \text{cls}(g), g \in T, \deg(g) = t-2\}.$$

The polynomials in  $T_1$  and  $T$  have different leading terms, hence  $T \cup T_1$  is a linearly independent basis of  $\ker M_{t-1}(y)$ . Moreover,  $T$  is a reduced basis of  $\ker M_{t-2}(y)$ , and  $T_1$  consists of all linearly independent polynomials with degree

$t - 1$  in  $\ker M_{t-1}(y)$ . We can deduce that the number of polynomials in  $T_1$  is equal to  $\text{corank } M_{t-1}(y) - \text{corank } M_{t-2}(y)$ . On the other hand, let  $\alpha_j$  denote the number of polynomials of class  $j$  and degree  $t - 2$  in  $T$ . Since the set  $T_1$  is constructed by multiplying polynomials in  $T$  of degree  $t - 2$  by their multiplicative variables only, the total number of polynomials in  $T_1$  is equal to  $\sum_{j=1}^n j\alpha_j$ . Therefore, the condition (10) is satisfied.  $\square$

**3.4. An Extension to  $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$ .** Consider the semialgebraic set  $\mathcal{A} := \{x \in \mathbb{R}^n \mid f_1(x) \geq 0, \dots, f_s(x) \geq 0\}$  and the  $\mathcal{A}$ -radical ideal  $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$ . We restrict to a subset  $\mathcal{K}_{t,\mathcal{A}} \subseteq \mathcal{K}_t$  defined as

$$\mathcal{K}_{t,\mathcal{A}} := \mathcal{K}_t \cap \left\{ y \in \mathbb{R}^{\mathbb{N}_{2t}^n} \mid M_{t-d_{f^\nu}}(f^\nu y) \succeq 0 \text{ for all } \nu \in \{0, 1\}^s \right\},$$

where  $d_{f^\nu} = \lceil \deg(f^\nu)/2 \rceil$  and  $t \geq d = \max_{1 \leq j \leq m, \nu \in \{0, 1\}^s} \{d_j, d_{f^\nu}\}$ .

For  $t$  large enough, Lemma 2.6 and Theorem 2.7 show that the information about  $\sqrt[t]{I}$  is contained in the projection of a generic element  $y \in \mathcal{K}_{t,\mathcal{A}}$ . Thus, propositions and theorems discussed above are true for generic elements  $y$  in  $\mathcal{K}_{t,\mathcal{A}}$ .

The following theorem can be seen as a variant of Theorem 3.1 for the semialgebraic set  $\mathcal{A}$ . The proof uses exactly the same reason as in Theorem 3.9 and Theorem 3.10 after replacing  $\mathcal{K}_t$  and  $\sqrt[t]{I}$  by  $\mathcal{K}_{t,\mathcal{A}}$  and  $\sqrt[t]{I}$  respectively.

**Theorem 3.11.** *Suppose the condition (10) holds for a generic element  $y \in \mathcal{K}_{t,\mathcal{A}}$ , and  $t \geq 2d$ . Then a reduced basis of the null space of  $M_{t-2}(y)$  is a weak Pommaret basis of  $\langle \ker M_{t-2}(y) \rangle$  under the monomial ordering  $\prec_{\text{tdeg}}$  and*

$$I \subseteq \langle \ker M_{t-2}(y) \rangle \subseteq I(V_{\mathbb{R}}(I) \cap \mathcal{A}).$$

**Remark 3.12.** For computing a Pommaret basis of  $\langle \ker M_{t-2}(y) \rangle$ , we add the defining polynomials  $\{f_1, \dots, f_s\}$  of the semialgebraic set  $\mathcal{A}$  to the input of the above algorithm and additional constraints  $M_{t-d_{f^\nu}}(f^\nu y) \succeq 0$  for all  $\nu \in \{0, 1\}^s$  to the semidefinite program (12).

#### 4. NUMERICAL EXAMPLES

We present here the results obtained by applying Algorithm 3.3 to some examples in [27, 30, 32, 36] and others.

**Example 4.1.** Consider the 2-dimensional ideal  $I = \langle h_1, h_2, h_3 \rangle$  taken from [36, p.397, Eq. (9.60)] where

$$\begin{aligned} h_1 &= x_1^2 + x_1x_2 - x_1x_3 - x_1 - x_2 + x_3, \\ h_2 &= x_1x_2 + x_2^2 - x_2x_3 - x_1 - x_2 + x_3, \\ h_3 &= x_1x_3 + x_2x_3 - x_3^2 - x_1 - x_2 + x_3. \end{aligned}$$

The rank and corank sequences for truncated moment matrices  $M_{t-\ell}(y)$  are shown in Table 1 and 2. We set  $\tau = 10^{-5}$  and  $x_1 \prec_{\text{tdeg}} x_2 \prec_{\text{tdeg}} x_3$ . For  $t=4$ , we have

$$\sum_{j=1}^3 j\alpha_j = 6, \text{ and } \text{corank } M_{4-1} - \text{corank } M_{4-2} = 6.$$

Hence, the condition (10) is satisfied. The Pommaret basis computed by Algorithm 3.3 for  $t = 4$  is

$$\{x_1 + x_2 - x_3 - x_1^2 - x_1x_2 + x_1x_3, x_1 + x_2 - x_3 - x_1x_2 - x_2^2 + x_2x_3, \\ 3x_1 + 3x_2 - 3x_3 - x_1^2 - 2x_1x_2 - x_2^2 + x_3^2\}.$$

From Table 3, we note that the condition (10) is also satisfied for  $t = 5, 6, 7$ . For this example, we can show that  $\langle \ker M_{4-2}(y) \rangle = \sqrt[3]{I}$ , and a reduced basis of  $\ker M_{4-2}(y)$  is a Pommaret basis of  $\sqrt[3]{I}$ . Hence, the condition (10) can be satisfied by arbitrary  $t \geq 4$ .

TABLE 1. The rank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	16	11	7
t=5	22	16	11
t=6	29	22	16
t=7	37	29	22

TABLE 2. The corank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	19	9	3
t=5	34	19	9
t=6	55	34	19
t=7	83	55	34

TABLE 3. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$ 

Order	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\sum_{j=1}^3 j\alpha_j$
t=4	1	1	1	$1 \times 1 + 1 \times 2 + 1 \times 3 = 6$
t=5	3	2	1	$3 \times 1 + 2 \times 2 + 1 \times 3 = 10$
t=6	6	3	1	$6 \times 1 + 3 \times 2 + 1 \times 3 = 15$
t=7	10	4	1	$10 \times 1 + 4 \times 2 + 1 \times 3 = 21$

**Example 4.2.** Consider the polynomial system  $P = \{h_1, h_2\}$  in [30, p.20, Ex 1.4.6], where

$$h_1 = x_1^2 - x_2, \\ h_2 = x_1x_2 - x_3.$$

For the term order  $x_3 \prec_{\text{tdeg}} x_1 \prec_{\text{tdeg}} x_2$ , we have  $\text{cls}(x_1) = 2$ ,  $\text{cls}(x_2) = 3$ ,  $\text{cls}(x_3) = 1$ . Let  $\tau = 10^{-8}$ , the rank and corank sequences for truncated moment matrices  $M_{t-\ell}(y)$  are shown in Table 4 and 5.

TABLE 4. The rank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=3	12	7	4
t=4	16	10	7
t=5	20	13	10

TABLE 5. The corank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=3	8	3	0
t=4	19	10	3
t=5	36	22	10

TABLE 6. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$ 

Order	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\sum_{j=1}^3 j\alpha_j$
t=3	0	0	0	$0 \times 2 + 0 \times 3 + 0 \times 1 = 0$
t=4	2	1	0	$2 \times 2 + 1 \times 3 + 0 \times 1 = 7$
t=5	3	1	3	$3 \times 2 + 1 \times 3 + 3 \times 1 = 12$

For t=4, we have

$$\sum_{j=1}^3 j\alpha_j = 7, \text{ and } \text{corank } M_{4-1} - \text{corank } M_{4-2} = 7.$$

Hence, the condition (10) is satisfied. The Pommaret basis computed by Algorithm 3.3 for  $t = 4$  is

$$\{x_1^2 - x_2, x_1x_2 - x_3, x_2^2 - x_1x_3\}.$$

**Example 4.3.** Consider the ideal  $I = \langle h_1, h_2 \rangle$  in [27, p.123, Ex 7.41] with

$$h_1 = x_1^2 + x_2^2 + x_3^2 - 2,$$

$$h_2 = x_1^2 + x_2^2 - x_3.$$

The real variety  $V_{\mathbb{R}}(I)$  for this ideal is strictly contained in  $V_{\mathbb{C}}(I)$ . We set  $\tau = 10^{-8}$  and  $x_1 \prec_{\text{tdeg}} x_2 \prec_{\text{tdeg}} x_3$ . The rank and corank sequences for truncated moment matrices  $M_{t-\ell}(y)$  are shown in Table 7 and 8.

TABLE 7. The rank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=3	7	5	3
t=4	9	7	5
t=5	11	9	7
t=6	13	11	9

TABLE 8. The corank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=3	13	5	1
t=4	26	13	5
t=5	45	26	13
t=6	71	45	26

TABLE 9. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$ 

Order	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\sum_{j=1}^3 j\alpha_j$
t=3	0	0	1	$0 \times 1 + 0 \times 2 + 1 \times 3 = 3$
t=4	1	2	1	$1 \times 1 + 2 \times 2 + 1 \times 3 = 8$
t=5	4	3	1	$4 \times 1 + 3 \times 2 + 1 \times 3 = 13$
t=6	8	4	1	$8 \times 1 + 4 \times 2 + 1 \times 3 = 19$

For t=4, we have

$$\sum_{j=1}^3 j\alpha_j = 8, \text{ and } \text{corank } M_{4-1} - \text{corank } M_{4-2} = 8.$$

Hence, the condition (10) is satisfied. The Pommaret basis computed by Algorithm 3.3 for  $t = 4$  is

$$\{-1 + x_3, -1 + x_1^2 + x_2^2\}.$$

For this example, we can show that  $\langle \ker M_{4-2}(y) \rangle = \sqrt[3]{I}$ , and a reduced basis of  $\ker M_{4-2}(y)$  is a Pommaret basis of  $\sqrt[3]{I}$ . Hence, the condition (10) can be satisfied by arbitrary  $t \geq 4$ .

**Example 4.4.** Consider the ideal  $I = \langle h_1, h_2, h_3 \rangle$  in [32, p.61, Ex 2.4.12], where

$$h_1 = x_3^2 + x_2x_3 - x_1^2,$$

$$h_2 = x_1x_3 + x_1x_2 - x_3,$$

$$h_3 = x_2x_3 + x_2^2 + x_1^2 - x_1.$$

Let  $\tau = 10^{-7}$  and the term order be  $x_1 \prec_{\text{tdeg}} x_2 \prec_{\text{tdeg}} x_3$ . The rank and corank sequences for the truncated moment matrices  $M_{t-\ell}(y)$  are shown in Table 10 and 11.

TABLE 10. The rank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	13	10	7
t=5	16	13	10
t=6	19	16	13
t=7	22	19	16

TABLE 11. The corank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	22	10	3
t=5	40	22	10
t=6	65	40	22
t=7	98	65	40

TABLE 12. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$ 

Order	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\sum_{j=1}^3 j\alpha_j$
t=4	1	1	1	$1 \times 1 + 1 \times 2 + 1 \times 3 = 6$
t=5	4	2	1	$4 \times 1 + 2 \times 2 + 1 \times 3 = 11$
t=6	8	3	1	$8 \times 1 + 3 \times 2 + 1 \times 3 = 17$
t=7	13	4	1	$13 \times 1 + 4 \times 2 + 1 \times 3 = 24$

The condition (10) can not be satisfied for  $t$  from 4 to 7. Actually, Seiler showed in [32] that the coordinates  $(x_1, x_2, x_3)$  are not  $\delta$ -regular for the ideal  $I$ . However, if we perform the linear transformation suggested in [32],  $\tilde{x}_1 = x_3$ ,  $\tilde{x}_2 = x_2 + x_3$ ,  $\tilde{x}_3 = x_1$ , after an auto-reduction, we obtain the polynomial system  $\tilde{P} = \{\tilde{x}_1\tilde{x}_2 - \tilde{x}_3^2, \tilde{x}_2\tilde{x}_3 - \tilde{x}_1, \tilde{x}_2^2 - \tilde{x}_3\}$ . We choose an ordering  $\tilde{x}_1 \prec_{\text{tdeg}} \tilde{x}_2 \prec_{\text{tdeg}} \tilde{x}_3$  and  $\tau = 10^{-8}$ . The rank and corank sequences for the truncated moment matrices  $M_{t-\ell}(y)$  are shown in Table 13 and 14.

For t=4, we have

$$\sum_{j=1}^3 j\alpha_j = 7, \text{ and } \text{corank } M_{4-1} - \text{corank } M_{4-2} = 7.$$



TABLE 13. The rank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	13	10	7
t=5	16	13	10
t=6	19	16	13

TABLE 14. The corank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=4	22	10	3
t=5	40	22	10
t=6	65	40	22

TABLE 15. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$ 

Order	$\alpha_1$	$\alpha_2$	$\alpha_3$	$\sum_{j=1}^3 j\alpha_j$
t=4	0	2	1	$0 \times 1 + 2 \times 2 + 1 \times 3 = 7$
t=5	3	3	1	$3 \times 1 + 3 \times 2 + 1 \times 3 = 12$
t=6	7	4	1	$7 \times 1 + 4 \times 2 + 1 \times 3 = 18$

Hence, the condition (10) is satisfied. The Pommaret basis computed by Algorithm 3.3 for  $t = 4$  is

$$\{-x_3 + x_2^2, -x_1 + x_2x_3, -x_1x_2 + x_3^2\}.$$

**Example 4.5.** Consider the ideal  $I = \langle h_1, h_2 \rangle$ , where

$$h_1 = (x_1 - x_2)(x_1 + x_2)^2(x_1 + x_2^2 + x_2),$$

$$h_2 = (x_1 - x_2)(x_1 + x_2)^2(x_1^2 + x_2^2).$$

In this example,  $I$  is not a radical ideal. We set  $\tau = 10^{-4}$  and  $x_1 \prec_{\text{tdeg}} x_2$ . The rank and corank sequences for the truncated moment matrices  $M_{t-\ell}(y)$  are shown in Table 16 and 17.

TABLE 16. The rank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=7	15	13	11
t=8	17	15	13
t=9	19	17	15

TABLE 17. The corank of  $M_{t-\ell}(y)$ 

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=7	21	15	10
t=8	28	21	15
t=9	36	28	21

TABLE 18. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$ 

Order	$\alpha_1$	$\alpha_2$	$\sum_{j=1}^2 j\alpha_j$
t=7	3	1	$3 \times 1 + 1 \times 2 = 5$
t=8	4	1	$4 \times 1 + 1 \times 2 = 6$
t=9	5	1	$5 \times 1 + 1 \times 2 = 7$

For t=7, we have

$$\sum_{j=1}^2 j\alpha_j = 5, \text{ and } \text{corank } M_{7-1} - \text{corank } M_{7-2} = 5.$$

Hence, the condition (10) is satisfied. The Pommaret basis computed by Algorithm 3.3 for  $t = 7$  is

$$\{-x_1^2 + x_2^2\}.$$

It should be noticed that for this example, if we set tolerance  $\tau < 10^{-4}$ , the rank and corank sequences for the truncated moment matrices  $M_{t-\ell}(y)$  will be completely different from those shown in Table 16 and 17, and we can not get  $\{-x_1^2 + x_2^2\}$  as a Pommaret basis of  $\sqrt[t]{I}$ .

**Example 4.6.** We compute  $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$  for  $I = \langle h_1, h_2 \rangle$ ,

$$h_1 = (x_1 - x_2)(x_1 + x_2)(x_1 + x_2^2 + x_2),$$

$$h_2 = (x_1 - x_2)(x_1 + x_2)(x_1^2 + x_2^2),$$

and

$$\mathcal{A} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 \geq 1, x_2 \geq 1\}.$$

Let us set  $\tau = 10^{-8}$  and  $x_1 \prec_{\text{tdeg}} x_2$ , the rank and corank sequences for the truncated moment matrices  $M_{t-\ell}(y)$  with  $y \in \mathcal{K}_{t,\mathcal{A}}$  are shown in Table 19 and 20.

TABLE 19. The rank of  $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=6	8	6	5
t=7	9	7	6
t=8	10	8	7

TABLE 20. The corank of  $M_{t-\ell}(y)$

Order	$\ell = 0$	$\ell = 1$	$\ell = 2$
t=6	20	15	10
t=7	27	21	15
t=8	35	28	21

TABLE 21. The  $\alpha_j$  of a reduced basis of  $\ker M_{t-2}(y)$

Order	$\alpha_1$	$\alpha_2$	$\sum_{j=1}^2 j\alpha_j$
t=6	3	1	$3 \times 1 + 1 \times 2 = 5$
t=7	4	1	$4 \times 1 + 1 \times 2 = 6$
t=8	5	1	$5 \times 1 + 1 \times 2 = 7$

For t=6, we have

$$\sum_{j=1}^2 j\alpha_j = 5, \text{ and } \text{corank } M_{6-1} - \text{corank } M_{6-2} = 5.$$

Hence, the condition (10) is satisfied. The Pommaret basis we obtain by Algorithm 3.3 for  $t = 6$  is

$$\{-x_1 + x_2\}$$

for  $I(V_{\mathbb{R}}(I) \cap \mathcal{A})$ .

## 5. CONCLUSION

In this paper we present a semidefinite characterization for computing a Pommaret basis of an ideal  $J$ , where  $J$  is generated by polynomials in the kernel of a truncated moment matrix and satisfies  $I \subseteq J \subseteq I(V_{\mathbb{R}}(I))$ . Our approach is stimulated by the previous work in [17, 18, 22, 26, 27, 29, 30, 32]. By combining the geometric involutive theory with the results on positive semidefinite moment matrices, we introduce a new stopping condition (10) for the semidefinite program (12) and prove the finite termination of the algorithm in a  $\delta$ -regular coordinate system. Although from the tables in Section 4, we can check that the condition (10) can be satisfied by higher order moment matrices once it is satisfied at some order, in general, we can not guarantee this property. Therefore, unlike flat extension conditions proposed by Curto and Fialkow in [8] for finite rank moment matrices, we can not prove the computed Pommaret basis is an involutive basis of the real radical ideal. Finally, we wish to mention that results computed by semidefinite programming and numerical linear algebra are approximate. Therefore, our condition (10) can only be checked with respect to a given tolerance. For improperly chosen tolerance, we might not be able to give a meaningful answer.

**Acknowledgement** We are most grateful to Jiawang Nie for many constructive remarks to improve the presentation of the paper. Yue Ma, Chu Wang and Lihong Zhi were partially supported by a NKBRPC 2011CB302400, and the Chinese National Natural Science Foundation under grant NSFC 91118001, 60911130369 and 60821002/F02.

## REFERENCES

- [1] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *J. Symb. Comput.*, 34(6):543–560, 2002.
- [2] B. Bank, M. Giusti, J. Heintz, and G.M. Mbakop. Polar varieties and efficient real elimination. *Math. Z.*, 238(1):115–144, 2001.
- [3] S. Basu, R. Pollack, and M.-F. Roy. On computing a set of points meeting every cell defined by a family of polynomials on a variety. *J. Complexity*, 13(1):28–37, 1997.
- [4] E. Becker and R. Neuhaus. Computation of real radicals of polynomial ideals. In *Computational algebraic geometry (Nice, 1992)*, volume 109 of *Progr. Math.*, pages 1–20. Birkhäuser Boston, Boston, MA, 1993.
- [5] E. Becker and T. Wörmann. Radical computations of zero-dimensional ideals and real root counting. *Math. Comput. Simulation*, 42(4-6):561–569, 1996. Symbolic computation, new trends and developments (Lille, 1993).
- [6] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.
- [7] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.
- [8] R. Curto and L. Fialkow. Solution of the truncated complex moment problem for flat data. *Memoirs of the American Mathematical Society*, 119(568):1–62, 1996.
- [9] D. Eisenbud, C. Huneke, and W. Vasconcelos. Direct methods for primary decomposition. *Invent. Math.*, 110(2):207–235, 1992.
- [10] Lawrence A. Fialkow. Solution of the truncated moment problem with variety  $y = x^3$ . *Trans. Amer. Math. Soc.*, 363:3133–3165, 2011.
- [11] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comput.*, 6(2/3):149–167, 1988.

- [12] D. Henrion and J.B. Lasserre. GloptiPoly: Global optimization over polynomials with Matlab and SeDuMi. *ACM Trans. Math. Softw.*, 29(2):165–194, 2003.
- [13] Ittuit Janovitz-Freireich, Bernard Mourrain, Lajos Rónyai, and Ágnes Szántó. On the computation of matrices of traces and radicals of ideals. *J. Symb. Comput.*, 47:102–122, January 2012.
- [14] T. Krick and A. Logar. An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 195–205. Springer, Berlin, 1991.
- [15] J.B. Lasserre. *Moments, Positive Polynomials and Their Applications*. Imperial College Press, 2009.
- [16] J.B. Lasserre, M. Laurent, B. Mourrain, P. Trébuchet, and P. Rostalski. Moment matrices, border bases and radical computation. Preprint, 2011.
- [17] J.B. Lasserre, M. Laurent, and P. Rostalski. Semidefinite characterization and computation of zero-dimensional real radical ideals. *Foundations of Computational Mathematics*, 8:607–647, 2008.
- [18] J.B. Lasserre, M. Laurent, and P. Rostalski. A prolongation-projection algorithm for computing the finite real variety of an ideal. *Theoretical Computer Science*, 410(27-29):2685–2700, 2009.
- [19] J.B. Lasserre, M. Laurent, and P. Rostalski. A unified approach to computing real and complex zeros of zero-dimensional ideals. In *Emerging applications of algebraic geometry*, volume 149 of *IMA Vol. Math. Appl.*, pages 125–155. Springer, New York, 2009.
- [20] M. Laurent. Revisiting two theorems of Curto and Fialkow on moment matrices. *Proceedings of the American Mathematical Society*, 133(10):2965–2976, 2005.
- [21] M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, volume 149 of *IMA Vol. Math. Appl.*, pages 157–270. Springer, New York, 2009.
- [22] M. Laurent and P. Rostalski. The approach of moments for polynomial equations. In Miguel F. Anjos and Jean B. Lasserre, editors, *Handbook on Semidefinite, Cone and Polynomial Optimization*, volume 166. Springer, 2010.
- [23] M. Marshall. *Positive polynomials and sums of squares*, volume 146 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2008.
- [24] H.M. Möller. An inverse problem for cubature formulae. *Computational Technologies*, 9(13-20), 2004.
- [25] R. Neuhaus. Computation of real radicals of polynomial ideals. II. *J. Pure Appl. Algebra*, 124(1-3):261–280, 1998.
- [26] G. Reid and L. Zhi. Solving polynomial systems via symbolic-numeric reduction to geometric involutive form. *J. Symbolic Comput.*, 44(3):280–291, 2009.
- [27] P. Rostalski. *Algebraic moments. real root finding and related topics*. PhD thesis, ETH Zurich, 2009.
- [28] M. Safey El Din and E. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings of the 16th international symposium on Symbolic and algebraic computation*, ISSAC '03, pages 224–231, New York, NY, USA, 2003. ACM.
- [29] R. Scott. *Approximate Gröbner Bases*. Master thesis, University of Western Ontario, Canada, 2006.
- [30] R. Scott, G. Reid, W. Wu, and L. Zhi. Geometric involutive bases and applications to approximate commutative algebra. In *Approximate commutative algebra*, Texts Monogr. Symbol. Comput., pages 99–124. SpringerWienNewYork, Vienna, 2009.
- [31] A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, 197:273–313, 1974.
- [32] W.M. Seiler. Involution - the formal theory of differential equations and its applications in computer algebra and numerical analysis. *Habilitation Thesis, Univ. of Mannheim*, 2002.
- [33] W.M. Seiler. *Involution: The Formal Theory of Differential Equations and its Applications in Computer Algebra*, volume 25 of *Algorithms and Computation in Mathematics*. Springer-Verlag, 2010.
- [34] S.J. Spang. *On the computation of the real radical*. Thesis, Technische Universität Kaiserslautern, 2007.

- [35] G. Stengle. A nullstellensatz and positivstellensatz in semialgebraic geometry. *Math. Ann.*, 207:87–97, 1994.
- [36] H.J. Stetter. *Numerical Polynomial Algebra*. SIAM, 2004.
- [37] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Rev.*, 38(1):49–95, 1996.
- [38] H. Wolkowicz, R. Saigal, and L. Vandenberghe, editors. *Handbook of Semidefinite Programming*. International Series in Operations Research & Management Science, 27. Kluwer Academic Publishers, Boston, MA, 2000. Theory, algorithms, and applications.
- [39] B. Xia and L. Yang. An algorithm for isolating the real solutions of semi-algebraic systems. *J. Symb. Comput.*, 34(5):461–477, 2002.
- [40] G. Zeng. Computation of generalized real radicals of polynomial ideals. *Sci. China Ser. A*, 42(3):272–280, 1999.